| **Corrigendum No. 1** | | | | | |
|---|---|---|---|---|---|
| Engagement of Cert-In empaneled agency for conducting Vulnerability Assessment & Penetration Testing and one round of revalidation of Intranet facing Web applications and mobile apps-Closed RFP | | | | | |
| **RFP No - SBI/GITC/Cyber Security/2025-2026/1399** | | | | | |
| **Pre-Bid Queries and Responses** | | | | | |
| **Sl. No** | **RFP Page No** | **RFP Clause No.** | **Existing Clause** | **Query/Suggestions** | **SBI responses** |
| 1 | 98 | 3 | Term of the Project – Project Schedule; Milestones and delivery locations | Will the activity be conducted in a hybrid model, fully onsite, or entirely remote? If onsite, please specify the number of locations involved and identify each location. | Full Onsite at bank premises |
| 2 | 53 | Appendix-E | DELIVERABLES/SCOPE OF WORK | Kindly confirm whether the associated infrastructure components of the applications are within the scope of assessment, or if the scope is limited to application-level testing only. If infrastructure is included, please provide the total number of assets to be considered | The scope is limited to as mentioned in the scope of work. VA perfomed will cover the Web server exposed to Desktops from where testing is being performed |
| 3 | 98 | 3 | Term of the Project – Project Schedule; Milestones and delivery locations | As security testing requires machines/devices with specific configurations (Rooted / Jailbroken Devices) and operating systems (Kali Linux), kindly confirm which party will be responsible for provisioning the necessary testing infrastructure, including the security testing workstation(s) for onsite activities. | A desktop connected to Intranet will be provided by the bank. Mobile device to be brought in by vendor.<br>Data in the mobile device to be wiped off after testing. Mobile device to be kept in the bank premises during engagement period. |

| | | | | | |
|---|---|---|---|---|---|
| 4 | Appendix-E (pp.53,55) | Appendix-E: Page 53: Description of Services<br><br>Appendix-E: Page 55:Description of Deliverables | Appendix-E: Page 53: Description of Services: To perform Vulnerability Assessment & Penetration testing on SBI Intranet facing Web Applications and Mobile apps of Bank with one round of revalidation. Testing should comprise<br><br>Appendix-E: Page 55:Description of Deliverables: No limit on confirmatory rounds. | Clarify scope for Revalidation : Please clarify whether the revalidation scope includes only one round of testing as mentioned on Page 53, or multiple confirmatory rounds as indicated on Page 55. | The RFP stands amended as:<br>Appendix-E: Page 53: Description of Services -<br>To perform Vulnerability Assessment & Penetration testing on SBI Intranet facing Web Applications and Mobile apps of Bank with no limit on the rounds of revalidation. |
| 5 | Appendix-E (pp.53) | Appendix-E: Page 53: Description of Services | Appendix-E: Page 53: Description of Services: APIs which are part of any Web or Mobile applications will also be a part of the respective scope of Web/Mobile Applications testing. | Clarify scope for Testing: Please clarity below points.<br>1. Kindly confirm the total number of API endpoints included in the testing scope.<br>2. Kindly confirm whether the API testing scope is limited to front-end APIs accessible from the browser, or also includes back-end APIs.<br>3. For mobile application testing, kindly confirm whether the mobile application APIs are to be tested independently or as part of the Gray box testing activity. | The APIs which are already integrated with the in-scope web/mobile apps will be included as part of testing.<br><br>Mobile application APIs are to be tested as part of the Grey box testing activity. |

| | | | | | |
|---|---|---|---|---|---|
| 6 | Appendix-E (pp.53) | Appendix-E: Page 53: Description of Services | Appendix-E: Page 53: Description of Services:<br>• Black Box Vulnerability Assessment & Penetration Testing of Intranet facing Web Applications: 65-75<br>• Grey Box Penetration Testing of Intranet facing Web Applications: 65-75<br>• Black Box Vulnerability Assessment & Penetration Testing of Intranet facing Mobile Applications: 1-10<br>• Grey Box Penetration Testing of Intranet facing Mobile Applications: 1-10 | Clarify scope for Testing:<br>1. Kindly confirm whether separate Black Box and Gray Box testing will be required for all applications covered under the mentioned scope.<br>2, Kindly Confirm if only dynamic testing will be part of the scope or static testing also will be in scope | 1. Yes.<br>Separate Blackbox & Greybox testing for all in-scope web & Mobile applications. Separate reports for Blackbox testing and Greybox testing to be provided.<br>2. Dynamic testing to be performed |
| 7 | Appendix-E (pp.56) | Appendix-E: Page 56: Payment schedule | Appendix-E: Page 56: Payment schedule:<br>1. 50% of total cost after completion of initial testing and submission of draft reports of all in scope Web application & Mobile application.<br>2. Remaining 50% of total cost after completion of the project and submission of all deliverables. | Clarify Sign off process:<br>1. Kindly confirm the sign off process for Draft report<br>2. Kindly provide final deliverables for project submission | Please abide by the published RFP |
| 8 | Appendix-E (pp.53) | Appendix-E: Page 53: Description of Services | Testing should be comprised of automatic (tool based) & detailed manual testing techniques. The report should be comprised of the testing checklist followed as per the latest OWASP guidelines. | kindly confirm whether the required automated security testing tools will be provided by SBI, or if it is expected that the bidder shall bring and utilize their own licensed tools for conducting the automated (tool-based) testing as per the scope | A desktop connected to Intranet will be provided by the bank. Vendor to bring in their own licensed tools for performing testing. |

| | | | | | |
|---|---|---|---|---|---|
| 9 | 53 | Appendix-E Description of Services | Indicative Scope of testing is placed below:<br>• Black Box Vulnerability Assessment & Penetration Testing of Intranet facing Web Applications: 65-75<br>• Grey Box Penetration Testing of Intranet facing Web Applications: 65-75<br>• Black Box Vulnerability Assessment & Penetration Testing of Intranet facing Mobile Applications: 1-10<br>• Grey Box Penetration Testing of Intranet facing Mobile Applications: 1-10 | Is there a list of specific web applications and mobile apps included in the scope?<br>This will help ensure that the exact applications to be tested are understood, and there are no misunderstandings about the scope. | Please abide by the RFP |
| 10 | 53 | Appendix-E Description of Services | APIs which are part of any Web or Mobile applications will also be a part of the respective scope of Web/Mobile Applications testing. | Please clarify the scope of API testing — specifically, whether the APIs to be tested are only those integrated with the in-scope web and mobile applications, and if so, kindly confirm whether the Bank will provide a list of such APIs along with details on any custom or standalone APIs that should be included in the testing. | The APIs which are already integrated with the in-scope web/mobile apps will be included as part of testing. |
| 11 | 53 | Appendix-E Description of Services | Testing should comprise of both Black Box (without credentials) and Grey Box (with user credentials) for all in-scope web & mobile applications. Testing should cover but not limited to the latest released OWASP | Please clarify whether the scope of testing includes Vulnerability Assessment of the servers hosting the in-scope web and mobile applications.<br>If yes, please confirm whether authenticated (credential-based) or unauthenticated (non-credential- | VA refers to the scanning of the Web servers which are reachable from the testing desktop. Authenticated scan to be performed. |

| | | | | | |
|---|---|---|---|---|---|
| | | | guidelines for Web, Mobile & APIs. | based) scans are expected to be performed. | |
| 12 | 53 | Appendix-E Description of Services | Both Black Box & Grey Box Testing of Web and Mobile applications to be conducted at Bank's premises under the supervision of bank officials. | Please confirm whether the Bank will provide the necessary testing infrastructure (such as desktops/laptops) required to perform both Black Box and Grey Box testing activities at the Bank's premises, or if the vendor's testing resources are expected to use their own devices within the Bank's environment. | A desktop connected to Intranet will be provided by the bank. |
| 13 | 53 | Appendix-E Description of Services | Testing should be comprised of automatic (tool based) & detailed manual testing techniques. | Will the Bank allow the installation and use open source security testing tools (e.g., OWASP ZAP, Nmap, Mobile Security Framework) on the provided systems? | A desktop connected to Intranet will be provided by the bank. Vendor to bring in their own licensed tools for performing testing. |
| 14 | 53 | Appendix-E Description of Services | Testing should be comprised of automatic (tool based) & detailed manual testing techniques. | For mobile application testing, will the Bank provide the required mobile devices or test environments (e.g., emulators, internal app stores, test credentials), or should the vendor arrange their own? | A desktop connected to Intranet will be provided by the bank. Mobile device to be brought in by vendor.<br>Data in the mobile device to be wiped off after testing. Mobile device to be kept in the bank premises during engagement period. |
| 15 | 53 | Appendix-E Description of Services | Both Black Box & Grey Box Testing of Web and Mobile applications to be conducted at Bank's premises under the supervision of bank officials. | Are there any specific working hours or access window restrictions for vendor resources during on-premises testing activities? | The testing activity should be performed in the presence of Bank official. |

| | | | | | |
|---|---|---|---|---|---|
| 16 | 53 | Appendix-E Description of Services | Revalidation of all the reported observation after confirmatory response from IT - AO | How will the revalidation process be conducted for previously reported vulnerabilities?<br>Will the revalidation of issues be carried out immediately after the fix or be part of a scheduled round?<br>For example:<br>If there are 10 observations reported during the initial VAPT, and the Bank's development team remediates 2 observations first while the others are still pending, should the vendor conduct revalidation immediately for those 2 observations, or wait until the remediation of all 10 observations is completed and perform one consolidated revalidation? | Revalidation to be conducted after the confirmation is received from IT-AOs that the mitigation is done. Confirmation testing to be done as and when the IT-AO performs the mitigation.<br>After the initial draft report is provided for any application, revalidation testing to be performed within next 3 months. |
| 17 | 54 | Appendix-E Description of Deliverables | Individual application wise (web & mobile) reports detailing the finding, | Please clarify the expected reporting format and structure for the deliverables. Should the VAPT findings be submitted as:<br>1. Individual reports for each application (separate reports for every web and mobile app),<br>2. Separate consolidated reports for all web applications and all mobile applications, or<br>3. A single consolidated report covering all web, mobile, and API components together? | Individual reports for each application.<br>And a consolidated report covering the whole scope of testing. |

| | | | | | |
|---|---|---|---|---|---|
| 18 | 56 | Appendix-E Term of the Project – Project Schedule; Milestones and delivery locations | Compiling all evidence and notes into a detailed report in Excel, Word and PPT that outlines findings including narrative of the overall attack path, the tactics used, the potential impact, Proof of Concept, steps to reproduce and recommendations for remediation of observations. | Please clarify whether the Bank requires the vendor to record vulnerabilities in any vulnerability tracking tool; if yes, kindly confirm whether the Bank has an existing tool for this purpose or if the vendor is expected to provide and manage one. | Bank has a vulnerability tracking tool. Vendor is expected to enter vulnerabilities within a week of publication of draft report in the tool and track the vulnerabilities to closure |
| 19 | 48 | Appendix-C Technical and Functional Specifications | The Bidder should have atleast 20 Offensive Security Certified Professional (OSCP) from offensive-security/ Certified Ethical Hacker (CEH) from EC-Council/ CompTIA Security+/ Licensed Penetration Tester (LPT) from EC-Council / GPEN: GIAC Penetration Tester from SANS/ GWAPT: GIAC Web Application Penetration Tester from SANS, as full-time employee. | Request you to also include other industry recognized penetration testing certifications. Please find below the ammmended clause including the additional certifications:<br><br>The Bidder should have atleast 20 Offensive Security Certified Professional (OSCP) from offensive-security/ Certified Ethical Hacker (CEH) from EC-Council/ CompTIA Security+/ Licensed Penetration Tester (LPT) from EC-Council / GPEN: GIAC Penetration Tester from SANS/ GWAPT: GIAC Web Application Penetration Tester from SANS/eJPT/eWPTx/eMAPT from INE , as full-time employee. | Please abide by the published RFP |

| | | | | | |
|---|---|---|---|---|---|
| 20 | 54 | Appendix-E Description of Deliverables | Final report should be submitted within 01 month of draft report. The report should be duly authorized and reviewed by management of service provider before submitted to the bank. | Will the final report include the confirmatory testing results? The confirmatory test results are largely dependent on the team fixing the observations and the time they take is outside our control. If they are not able to fix all observations within 1 month then it may not be possible to submit the final report within 1 month. | Yes.<br>After the initial draft report is provided for any application, revalidation testing to be performed within next 3 months. |
| 21 | 54 | Appendix-E Description of Deliverables | Period of engagement will be 06 months | Our understanding is that the entire engagement including initial testing and confirmatory testing will be for 6 months. Post 6 months there will be no further testing, including an confirmatory rounds. Please let us know in case our understanding is wrong. | After the initial draft report is provided for any application, revalidation testing to be performed within next 3 months. |